

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004 年 2 月 19 日 (19.02.2004)

PCT

(10) 国際公開番号
WO 2004/015916 A1

(51) 国際特許分類: H04L 9/06, G09C 1/00

(21) 国際出願番号: PCT/JP2003/010186

(22) 国際出願日: 2003 年 8 月 8 日 (08.08.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-231284 2002 年 8 月 8 日 (08.08.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電
器産業株式会社 (MATSUSHITA ELECTRIC INDUS-
TRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市
大字門真 1 0 0 6 番地 Osaka (JP).

(FUKUOKA, Toshihiko) [JP/JP]; 〒575-0061 大阪府
四条畷市 清滝中町 1 5-2 4 Osaka (JP). 和田 妙美
(WADA, Taemi) [JP/JP]; 〒572-0013 大阪府 寝屋川市
三井が丘 4-4-8 2-4 0 6 Osaka (JP).

(74) 代理人: 前田 弘, 外 (MAEDA, Hiroshi et al.); 〒550-
0004 大阪府 大阪市 西区鞠本町 1 丁目 4 番 8 号 本町
中島ビル Osaka (JP).

(81) 指定国 (国内): CN, JP, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY,
CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC,
NL, PT, RO, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

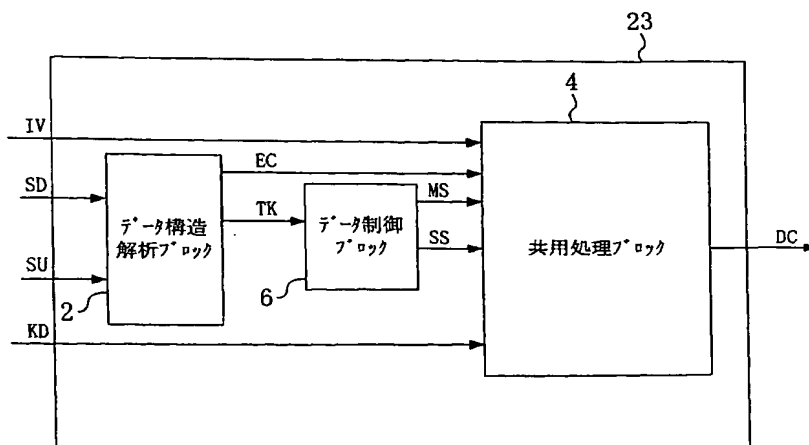
2 文字コード及び他の略語については、定期発行される
各 PCT ガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 福岡 俊彦

(54) Title: ENCRYPTING/DECRYPTING DEVICE AND METHOD, ENCRYPTING DEVICE AND METHOD, DECRYPTING
DEVICE AND METHOD, AND TRANSMITTING/RECEIVING DEVICE

(54) 発明の名称: 暗号化復号化装置及び方法、暗号化装置及び方法、復号化装置及び方法、並びに送受信装置



2... DATA STRUCTURE ANALYZING BLOCK

6... DATA CONTROL BLOCK

4... SHARED PROCESSING BLOCK

(57) Abstract: An encrypting/decrypting device comprises a data structure analyzing block that receives encrypted data or data to be encrypted and that outputs, as processing-block input data, control data and the encrypted data or data to be encrypted; a data control block that obtains and outputs a mode selection signal in accordance with the control data; and a shared processing block that encrypts or decrypts the processing-block input data and outputs the resultant. The shared processing block is adapted to perform an ECB processing using input key data so that it can perform encryption and decryption in any one of CBC and CFB modes. The shared processing block, therefore, performs an encryption or decryption in a mode indicated by the mode selection signal.

[続葉有]



(57) 要約: 暗号化復号化装置として、暗号化データ又は暗号化すべきデータを受け取り、制御用データ、及び、暗号化データ又は暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、制御用データに従ってモード選択信号を求めて出力するデータ制御ブロックと、処理ブロック入力データに対して暗号化又は復号化を行い、得られた結果を出力する共用処理ブロックとを備える。共用処理ブロックは、入力された鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、モード選択信号に示されたモードで暗号化又は復号化を行う。

明 細 書

暗号化復号化装置及び方法、暗号化装置及び方法、復号化装置及び方法、並びに
送受信装置

技術分野

本発明は、暗号化及び暗号の復号化技術に関する。

背景技術

デジタル双方向通信の代表的な例である双方向CATV (cable television) システムでは、暗号化機能を実現するために、TV端末には暗号化機能が実装される。この暗号化機能としては、DES (data encryption standard) 暗号に代表される秘密鍵暗号方式と、RSA (Rivest-Shamir-Adleman) 暗号に代表される公開鍵暗号方式とを組み合わせた方式が用いられる。

秘密鍵暗号方式とは、暗号化と復号化とに用いる鍵が共通であり、暗号化に用いられた鍵を用いて暗号化アルゴリズムを逆の順に実行することによって復号化を行い、暗号化を施す前の原文を得る方式である。この方式は、単純な排他的論理和の繰り返しアルゴリズムで実現されるもので、高速な処理を可能とする反面、送信側と受信側とで共通の鍵を保有する必要があるため、鍵の配送・保持が困難であるという特徴を有する。

公開鍵暗号方式とは、落とし戸関数と呼ばれる、関数の演算は容易に実行でき、逆関数の演算を行うのは非常に困難であるような関数を利用するものであり、暗号化と復号化とに使用する鍵が異なるものである。したがって、鍵の配送・保持は容易に行える反面、秘密鍵暗号方式に比べて計算が複雑であり、秘密鍵暗号方式と比較して暗号化・復号化により多くの処理時間を要する。ただし、公開鍵暗号方式を使用して認証及び鍵配送を行い、秘密鍵暗号方式を使用してデータの暗

号化を行うことによって、それぞれの利点を生かすことが可能となる。

さて、米国の標準方式であるDES暗号方式では、ECB (electronic code book) モードと呼ばれる、入力データサイズが64ビット、出力データサイズが64ビットの演算を基本処理として行う。この暗号方式の暗号化アルゴリズムに対して、あらかじめ文字又は単語が出現する頻度の分布を統計処理しておけば、入手した暗号化文の文字列パターンの頻度分布とのマッチングをとることにより、暗号化前の平文が推定されてしまう可能性がある。

そこで、暗号化された64ビットの暗号ブロックと次に入力される64ビットの入力データとの排他的論理和を演算して暗号文を作成する方法が考え出された。この方法を行って暗号化するモードをCBC (cipher block chaining) モードと呼んでいる。また、パケット通信のように通信を行う際のデータ単位があらかじめ決められている場合があるが、64ビットを1ブロックとするブロック暗号化方式では、1ブロックのビット数(64ビット)で割り切れないデータ単位が入力された場合には、1ブロックに満たない端数データができる。

データに端数部分がある場合には、1つ前のブロックの暗号解読演算結果と端数データの排他的論理和演算を実行し暗号化する。このような端数処理を行うモードの1つとして、CFB (cipher feedback) モードがあり、CFBモードによって、データが64ビットに満たない場合でも暗号文を得ることができる。

また、暗号化及び暗号解読(復号化)のいずれの演算においても、通常は56ビットのデータを鍵として用いるが、特定の条件下では、40ビットのデータを鍵として用いるモードも存在する。この場合、他のモードの場合と同様に、演算処理自体は64ビット単位で行うが、鍵の有効データが40ビットとなる。

このように、秘密鍵暗号方式演算においては複数のモード、すなわち、ECBモード、CBCモード及びCFBモードのうちの1つと、56ビット鍵モード又は40ビット鍵モードのいずれかとの組み合わせに対応したモードが存在する。そして、デジタル双方向通信のセキュリティ機能を実現するために、すべてのモードに対応した暗号化装置又は復号化装置が一般的に用いられる。

関連する技術が、例えば米国特許第 5, 8 3 5, 5 9 9 号明細書に開示されている。

－解決課題－

従来の D E S 暗号方式に基づく暗号化装置又は復号化装置は、複数のモードのそれぞれのための回路を備え、システムの要求に応じて複数のモードのいずれかを適宜選択し、そのモードのための回路を用いて暗号化演算又は暗号解読演算を行う構成となっている。

ところが、近年、暗号化又は暗号解読を必要とするシステムでは、単一の鍵のみを使用する場合は少なく、複数の鍵を使用して、それぞれの鍵に対応した演算を行う場合も増加してきている。

これを実現する装置は、各モードごとの暗号化又は暗号解読機能を備えた上、複数の鍵に対する演算を行う機能も必須となり、回路規模は莫大なものとなる。一般的に、複数の鍵に対する演算は並列実行する必要があるため、処理が必要となる鍵の数が増大すると、装置としても、鍵の数に応じた数の処理回路を有する必要がある。

しかし、D E S の各モードは、E C B 処理と呼ばれる、D E S の基本処理を変形した処理が行われるものである。また、各モードを同時に並列実行する場合はほとんどない。このため、暗号化装置及び復号化装置において、複数のモードで処理回路を共用化して回路規模を削減することは可能である。

発明の開示

本発明は、複数の暗号モードで処理回路を共用化することによって、回路規模を削減した暗号化復号化装置、暗号化装置、復号化装置、及び送受信装置を提供することを目的とする。

本発明の暗号化復号化装置は、暗号化データ又は暗号化すべきデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロッ

ク入力データとして出力するデータ構造解析ブロックと、前記制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、前記処理ブロック入力データに対して前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する共用処理ブロックとを備え、前記共用処理ブロックは、入力された鍵データを用いたE C B (electronic code book) 処理を行うことによって、C B C (cipher block chaining) モード及びC F B (cipher feedback) モードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化又は復号化を行うものである。

これによると、複数の暗号モードでの暗号化及び復号化の処理を共用処理ブロックによって実現することができるので、暗号モード毎に処理回路を設ける必要がない。したがって、暗号化復号化装置の回路面積を削減して、そのコストを抑えることができる。

また、本発明の暗号化装置は、暗号化すべきデータを受け取り、そのデータ構造の解析を行って、制御用データを求めて出力するとともに、前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、前記処理ブロック入力データに対して暗号化を行い、得られた暗号化結果を出力する共用処理ブロックとを備え、前記共用処理ブロックは、入力された鍵データを用いたE C B 処理を行うことによって、C B C モード及びC F B モードのいずれにおいても暗号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化を行うものである。

また、本発明の復号化装置は、暗号化データを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記

暗号化データを処理ブロック入力データとして出力するデータ構造解析ブロックと、前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、前記処理ブロック入力データに対して復号化を行い、得られた復号化結果を出力する共用処理ブロックとを備え、前記共用処理ブロックは、入力された鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで復号化を行うものである。

また、本発明の送受信装置は、受信した信号をデータに変換して出力するダウンストリームPHY部と、前記データからダウンストリームデータ及び鍵データを分離して出力するダウンストリームデータ処理部と、前記鍵データを用いて前記ダウンストリームデータを復号化して出力する第1の暗号化復号化装置と、前記復号化されたダウンストリームデータを格納する記憶部と、前記記憶部から読み出されたアップストリームデータを暗号化して出力する第2の暗号化復号化装置と、前記暗号化されたアップストリームデータに、暗号化に用いられた鍵データを付加して出力するアップストリームデータ処理部と、前記アップストリームデータ処理部が出力するデータを信号に変換して送信するアップストリームPHY部とを備え、前記第1及び第2の暗号化復号化装置は、いずれも、暗号化データを含む前記ダウンストリームデータ又は暗号化すべきデータを含む前記アップストリームデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、前記制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、前記処理ブロック入力データに対して前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する共用処理ブ

ロックとを有するものであり、前記共用処理ブロックは、入力された鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化又は復号化を行うものである。

－発明の効果－

以上のように、本発明によると、同一のハードウェアによって多くの暗号モードにおいて暗号化／復号化を行うことができるので、回路面積を削減してコストを抑えることができる。多くの機能を低コストで提供することができるので、暗号化復号化装置等のコストパフォーマンスを高めることができる。

図面の簡単な説明

図1は、本発明の実施形態に係る暗号化復号化装置の構成を示すブロック図である。

図2は、図1の共用処理ブロックの構成の例を示すブロック図である。

図3は、図1の共用処理ブロックが行う処理の流れを示す説明図である。

図4は、図1の共用処理ブロックの第1～第4のセレクタが選択するデータの組み合わせを示す説明図である。

図5は、本発明の実施形態に係る暗号化復号化装置の他の構成の例を示すブロック図である。

図6は、図1の暗号化復号化装置を用いた送受信装置のブロック図である。

発明を実施するための最良の形態

以下、本発明の実施の形態について、図面を参照しながら説明する。

図1は、本発明の実施形態に係る暗号化復号化装置の構成を示すブロック図である。図1の暗号化復号化装置23は、データ構造解析ブロック2と、共用処理ブロック4と、データ制御ブロック6とを備えている。以下では例として、図1の暗号化復号化装置23は、センター装置及び複数の端末装置により構成される

双方向通信網において、端末装置の１つに含まれるものであるとして説明するが、センター装置に含まれていてもよい。センター装置は、暗号化されたデータを含むダウンストリームデータSDを端末装置に送信する。ダウンストリームデータSDには、映像データ及び伝送制御データが含まれている。一方、端末装置は、暗号化すべきデータを含むアップストリームデータを受け取り、暗号化してセンター装置に対して送信する。

データ構造解析ブロック２は、ダウンストリームデータSDを受け取り、その構文解析を行う。ダウンストリームデータSDは、例えば、映像データにおけるMPEG (moving picture experts group) 構造と、MPEG構造に埋め込まれているネットワーク処理用のサブレイヤであるMAC (media access control) 構造を有している。

まず、データ構造解析ブロック２は、MPEG構造データ中のヘッダ部分を解析し、MAC構造データを抜き出すための情報を抽出した後に、MAC構造データを抜き出す。次に、MAC構造データ中のヘッダ部分を解析し、通常のヘッダのみでなく、拡張ヘッダと呼ばれる拡張されたフィールドが存在する場合は、この拡張ヘッダを解析する。拡張ヘッダは、データ構成の拡張を可能にするものであって、暗号化の有無、その他の暗号化又は復号化のための処理に必要となる情報を有している。

拡張ヘッダが存在しない場合、データ構造解析ブロック２は、ダウンストリームデータSDが暗号化されていないと判断する。この場合、データ構造解析ブロック２は、TEK (traffic encryption key) 制御用データTKを例えば値“０”に固定し、データ制御ブロック６に出力する。

拡張ヘッダが存在する場合、データ構造解析ブロック２は、暗号化に関する情報を格納するフィールドを解析する。暗号化されていないことを確認した場合には、拡張ヘッダが存在しない場合と同様の処理を行う。暗号化されていることを確認した場合には、暗号化に関する情報であるSID (service ID) 及びキーシーケンスナンバー (key sequence number) を拡張ヘッダから抽出し、TEK制

御用データTKとしてデータ制御ブロック6に出力する。

また、データ構造解析ブロック2は、暗号化すべきデータをアップストリームデータSUとして受け取り、そのデータ構造の解析を行う。データ構造解析ブロック2は、アップストリームデータSUに含まれるデータからSID及びキーシーケンスナンバーを抽出し、TEK制御用データTKとしてデータ制御ブロック6に出力する。

データ構造解析ブロック2は、ダウンストリームデータSDに含まれるMPERG構造を有する暗号化データ、又はアップストリームデータSUに含まれる暗号化すべきデータを、処理ブロック入力データECとして共用処理ブロック4に出力する。

データ構造解析ブロック2は、受信したダウンストリームデータSD又はアップストリームデータSUのパケットのビット数をカウントし、ストリームのパケットのビット数が64ビット以下、64ビットの倍数、又は64ビットの倍数と64ビット以下の端数との和のいずれであるか、及びパケットのうち処理ブロック入力データECとして出力したビット数（パケットカウント）を求める。データ構造解析ブロック2は、求められた結果、並びに、ダウンストリームデータSDを受け取った場合には復号化すべきであることを、及びアップストリームデータSUを受け取った場合には暗号化すべきであることをもTEK制御用データTKとしてデータ制御ブロック6に出力する。

次に、データ制御ブロック6は、データ構造解析ブロック2から受信したTEK制御用データTKを用いて処理を行う。まず、SID及びキーシーケンスナンバーをチェックして、これらのデータがあらかじめ決められている有効な数値であるかどうかを判断する。無効な数値であると判断した場合は、何も処理を行わない。有効な数値であると判断した場合は、データ制御ブロック6は、56ビット鍵モードであるか否かをチェックする。暗号化及び復号化には、56ビットの鍵が標準として用いられるが、これ以外の長さの鍵も用いられる。以下では例として、56ビット又は40ビットの鍵が用いられるものとする。56ビット鍵モ

ードであるか否かは、S I D及びキーシーケンスナンバーに一意に対応する。データ制御ブロック 6 は、5 6 ビット鍵モードであるか否かを示す情報をモード選択信号MSとして出力する。

データ制御ブロック 6 は、T E K制御用データTKに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号S Sを共用処理ブロック 4 に出力する。また、データ制御ブロック 6 は、T E K制御用データTKを参照して、処理ブロック入力データE Cのパケットのビット数が6 4 ビット以下の場合はC F Bモードを示す信号を、6 4 ビットの倍数である場合はC B Cモードを示す信号を、モード選択信号MSとして共用処理ブロック 4 に出力する。

パケットのビット数が6 4 ビットの倍数と6 4 ビット以下の端数との和である場合は、データ制御ブロック 6 は、パケットカウントに応じて、モード選択信号MSを次のように切り替える。すなわち、データ構造解析ブロック 2 が6 4 ビットの倍数に相当する処理ブロック入力データE Cを出力しているときは、C B Cモードを示す信号を、6 4 ビット以下の端数に相当する処理ブロック入力データE Cを出力しているときは、C F Bモードを示す信号を、データ制御ブロック 6 がモード選択信号MSとして出力する。また、データ制御ブロック 6 は、それぞれのモードの処理を開始する初期状態、又はその後の定常状態のいずれであるかも、モード選択信号MSとして出力する。

また、データ構造解析ブロック 2 は、受信したダウンストリームデータS D又はアップストリームデータS Uに応じて、E C Bモードで処理すべきか否かをT E K制御用データTKによってデータ制御ブロック 6 に通知する。E C Bモードで処理すべき場合には、データ制御ブロック 6 は、E C Bモードを示す信号をモード選択信号MSとして出力する。

このように、データ制御ブロック 6 は、S I D、キーシーケンスナンバー、及びパケットカウント等に応じてモード選択信号MSを切り替えて、共用処理ブロック 4 に出力する。

共用処理ブロック 4 は、複数の暗号モードにおける処理に共通に用いられる。

すなわち、共用処理ブロック 4 は、外部から入力された初期ベクタデータ I V、及び鍵データ K Dを用いた E C B 処理を行うことによって、E C B モード、C B C モード及び C F B モードのいずれの暗号モードにおいても、処理ブロック入力データ E C に対して暗号化及び復号化を行うことができるように構成されている。共用処理ブロック 4 は、モード選択信号 M S に示されたモードで、暗号化／復号化切り替え信号 S S に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を処理済データ D C として出力する。

図 2 は、図 1 の共用処理ブロック 4 の構成の例を示すブロック図である。図 2 の共用処理ブロック 4 は、第 1 のセレクトア 4 1 と、第 2 のセレクトア 4 2 と、第 3 のセレクトア 4 3 と、第 4 のセレクトア 4 4 と、ビットマスク器 4 6 と、E C B 処理器 4 7 と、遅延器 4 8 と、排他的論理和演算器 4 9 とを備えている。

第 1 のセレクトア 4 1 は、暗号化／復号化切り替え信号 S S 及びモード選択信号 M S に従って、処理ブロック入力データ E C、及び E C B 処理器 4 7 が出力する暗号処理データ P D のうちのいずれかを選択して排他的論理和演算器 4 9 に出力する。

遅延器 4 8 は、処理ブロック入力データ E C、及び暗号処理データ P D を入力とし、それぞれを、E C B 処理器 4 7 が 6 4 ビットのデータに対して E C B 処理を行うのに要する時間だけ遅延させて、第 2 のセレクトア 4 2 に出力する。

第 2 のセレクトア 4 2 は、暗号化／復号化切り替え信号 S S 及びモード選択信号 M S に従って、処理ブロック入力データ E C、初期ベクタデータ I V、並びに、遅延器 4 8 が出力する遅延した処理ブロック入力データ E C D 及び遅延した暗号処理データ P D D のうちのいずれかを選択して排他的論理和演算器 4 9 に出力する。

排他的論理和演算器 4 9 は、第 1 のセレクトア 4 1 の出力と第 2 のセレクトア 4 2 の出力との排他的論理和を対応するビット毎に求めて第 4 のセレクトア 4 4 に出力する。

第 3 のセレクトア 4 3 は、暗号化／復号化切り替え信号 S S 及びモード選択信号

MSに従って、処理ブロック入力データEC、排他的論理和演算器49が出力する排他的論理和データER、遅延した処理ブロック入力データECD、及び遅延した暗号処理データPDDのうちのいずれかを選択してECB処理器47に出力する。

ビットマスク器46は、鍵データKDを、モード選択信号MSに従って必要に応じてその一部をマスクして、モードに適合した鍵データとしてECB処理器47に出力する。

第4のセクタ44は、暗号化／復号化切り替え信号SS及びモード選択信号MSに従って、暗号処理データPD及び排他的論理和演算器49が出力する排他的論理和データERのうちのいずれかを選択して、暗号化結果又は復号化結果として出力する。

ECB処理器47は、暗号化／復号化切り替え信号SS及びモード選択信号MSに従って、ECB処理として暗号化処理及び復号化処理のうちのいずれかを、第3のセクタ43の出力に対して行う。ECB処理器47は、ビットマスク器46が出力するモードに適合した鍵データを用いてECB処理を行い、得られた結果を暗号処理データPDとして第1のセクタ41、第4のセクタ44、及び遅延器48に出力する。

図3は、図1の共用処理ブロック4が行う処理の流れを示す説明図である。図3において、上段は暗号化処理の流れを示し、下段は復号化処理の流れを示している。処理E1、E2、E3、E9、D1、D2、D3、D9はそれぞれECB処理を表している。共用処理ブロック4は、暗号化処理及び復号化処理のいずれの場合にも、CBCモードによる処理を行う必要があるときは、CBCモードによる処理を連続して行い、その後、必要に応じてCFBモードによる処理を行う。

図3では、処理E9、D9を含む最も右の列の処理はCFBモードの処理を示している。処理E1、E2、E3、D1、D2、D3を含むその他の3つの列の処理はCBCモードの処理を示している。また、「IV」は初期ベクタデータ、「D」は暗号化されていないデータ、「I」は、図3上段の暗号化処理の場合は

ECB処理前、下段の復号化処理の場合はECB処理後のデータを示す。また、「C」は暗号化データ、「Encrypt」はECB処理器47におけるECB処理が暗号化処理であること、「Decrypt」はECB処理器47におけるECB処理が復号化処理であることを示す。実際のECB処理には鍵データを用いるが、図3においては、鍵データのデータフローは省略している。図3の処理の流れは、56ビット鍵モードであるか否かにかかわらず同様である。

図4は、図1の共用処理ブロック4の第1～第4のセレクタ41～44が選択するデータの組み合わせを示す説明図である。共用処理ブロック4の復号化処理時の動作について、図2、図3の下段、及び図4を参照して説明する。この場合、共用処理ブロック4には、暗号化／復号化切り替え信号SSとして、復号化を示す信号が入力される。56ビット鍵モードであるか否か、CBCモード及びCFBモードのうちのいずれであるか、初期状態及び定常状態のうちのいずれであるかによって場合を分けて説明する。ECB処理器47におけるECB処理は、CBCモードの場合は復号化処理、CFBモードの場合は暗号化処理である。

1) 56ビット鍵モードであり、かつ、CBCモードの初期状態である場合
(図4のDEC-CBC Initの場合)

この場合は、図3の下段の処理D1及びこれに続く排他的論理和を求める処理が行われる。共用処理ブロック4は、暗号化データCを入力とし、ECB処理として「Decrypt」処理を行って、データIを求める。共用処理ブロック4は、求められたデータIと入力された初期ベクタデータIVとの排他的論理和を求めて、暗号化されていないデータDとして出力する。

この場合の処理を、図2を参照して説明する。共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードであること、及びCBCモードの初期状態であることを示す信号が入力される。

第1のセレクタ41は、ECB処理器47が出力する暗号処理データPDを選択して出力する。第2のセレクタ42は、初期ベクタデータIVを選択して出力する。排他的論理和演算器49は、暗号処理データPDと初期ベクタデータIV

との排他的論理和を対応するビット毎に求め、得られた排他的論理和データ E R を出力する。

第3のセクタ43は、処理ブロック入力データ E C を選択して E C B 処理器 47 に出力する。ビットマスク器 46 は、モード選択信号 M S として 56 ビット鍵モードであることを示す信号が入力されているので、入力された 56 ビットの鍵データ K D をマスクせずにそのまま E C B 処理器 47 に出力する。

E C B 処理器 47 は、ビットマスク器 46 から出力された 56 ビット鍵データを用いて、第3のセクタから出力された処理ブロック入力データ E C に対して E C B 処理として復号化処理を行い、得られた暗号処理データ P D を出力する。第4のセクタは、排他的論理和演算器 49 が出力する排他的論理和データ E R を選択して、処理済データ D C として復号化結果を出力する。

2) 56 ビット鍵モードであり、かつ、C B C モードの定常状態である場合 (図4の D E C - C B C N o r m a l の場合)

この場合は、図3の下段の処理 D 2 又は D 3 及びこれらのそれぞれに続く排他的論理和を求める処理が行われる。共用処理ブロック 4 は、暗号化データ C を入力とし、「D e c r y p t」処理を行って、データ I を求める。共用処理ブロック 4 は、求められたデータ I とその前の E C B 処理で用いた暗号化データ C との排他的論理和を求めて、暗号化されていないデータ D として出力する。

この場合の処理を、図2を参照して説明する。共用処理ブロック 4 には、モード選択信号 M S として、56 ビット鍵モードであること、及び C B C モードの定常状態であることを示す信号が入力される。

第1のセクタ41は、E C B 処理器 47 が出力する暗号処理データ P D を選択して出力する。第2のセクタ42は、遅延器 48 が出力する遅延された処理ブロック入力データ E C D を選択して出力する。排他的論理和演算器 49 は、暗号処理データ P D と遅延された処理ブロック入力データ E C D との排他的論理和を対応するビット毎に求め、得られた排他的論理和データ E R を出力する。

第3のセクタ43は、処理ブロック入力データ E C を選択して E C B 処理器

47に出力する。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードであることを示す信号が入力されているので、入力された56ビットの鍵データKDをマスクせずにそのままECB処理器47に出力する。

ECB処理器47は、ビットマスク器46から出力された56ビット鍵データを用いて、第3のセクタから出力された処理ブロック入力データECに対してECB処理として復号化処理を行い、得られた暗号処理データPDを出力する。第4のセクタは、排他的論理和演算器49が出力する排他的論理和データERを選択して、処理済データDCとして復号化結果を出力する。

3) 56ビット鍵モードではなく、かつ、CBCモードの初期状態である場合

4) 56ビット鍵モードではなく、かつ、CBCモードの定常状態である場合

これらの場合は、それぞれ1), 2)の場合と次の点を除いて同じである。すなわち、共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードではないことを示す信号が入力される。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードではないことを示す信号が入力されているので、入力された56ビットの鍵データKDのうち、必要がないビット（例えば上位16ビット）をマスクして、40ビット鍵データとしてECB処理器47に出力する。ECB処理器47は、ビットマスク器46から出力された40ビット鍵データを用いてECB処理を行う。

5) 56ビット鍵モードであり、かつ、CFBモードの初期状態である場合
(図4のDEC-CFB Initの場合)

CFBモードの処理のみを行うときには、CFBモードの初期状態における処理が行われる。この場合は、図3の下段の処理D9及びこれに続く排他的論理和を求める処理が行われる。共用処理ブロック4は、暗号化データCを入力とし、「Encrypt」処理を行って、データIを求める。共用処理ブロック4は、求められたデータIと入力された初期ベクタデータIVデータとの排他的論理和を求めて、暗号化されていないデータDとして出力する。

この場合の処理を、図2を参照して説明する。共用処理ブロック4には、モー

ド選択信号MSとして、56ビット鍵モードであること、及びCFBモードの初期状態であることを示す信号が入力される。

第1のセレクタ41は、ECB処理器47が出力する暗号処理データPDを選択して出力する。第2のセレクタ42は、初期ベクタデータIVを選択して出力する。排他的論理和演算器49は、暗号処理データPDと初期ベクタデータIVとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データERを出力する。

第3のセレクタ43は、処理ブロック入力データECを選択してECB処理器47に出力する。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードであることを示す信号が入力されているので、入力された56ビットの鍵データKDをマスクせずにそのままECB処理器47に出力する。

ECB処理器47は、ビットマスク器46から出力された56ビット鍵データを用いて、第3のセレクタから出力された処理ブロック入力データECに対してECB処理として暗号化処理を行い、得られた暗号処理データPDを出力する。第4のセレクタは、排他的論理和演算器49が出力する排他的論理和データERを選択して、処理済データDCとして復号化結果を出力する。

6) 56ビット鍵モードであり、かつ、CFBモードの定常状態である場合
(図4のDEC-CFB Normalの場合)

CBCモードの処理に続いてCFBモードの処理を行うときには、CFBモードの定常状態における処理が行われる。この場合は、図3の下段の処理D9及びこれに続く排他的論理和を求める処理が行われる。共用処理ブロック4は、その前のECB処理で用いた暗号化データCを入力とし、「Encrypt」処理を行って、データIを求める。共用処理ブロック4は、求められたデータIと次の暗号化データCとの排他的論理和を求めて、暗号化されていないデータDとして出力する。

この場合の処理を、図2を参照して説明する。共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードであること、及びCFBモードの定

常状態であることを示す信号が入力される。

第1のセレクタ41は、ECB処理器47が出力する暗号処理データPDを選択して出力する。第2のセレクタ42は、処理ブロック入力データECを選択して出力する。排他的論理和演算器49は、暗号処理データPDと処理ブロック入力データECとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データERを出力する。

第3のセレクタ43は、遅延器48が出力する遅延された処理ブロック入力データECDを選択してECB処理器47に出力する。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードであることを示す信号が入力されているので、入力された56ビットの鍵データKDをマスクせずにそのままECB処理器47に出力する。

ECB処理器47は、ビットマスク器46から出力された56ビット鍵データを用いて、第3のセレクタから出力された遅延された処理ブロック入力データECDに対してECB処理として暗号化処理を行い、得られた暗号処理データPDを出力する。第4のセレクタは、排他的論理和演算器49が出力する排他的論理和データERを選択して、処理済データDCとして復号化結果を出力する。

7) 56ビット鍵モードではなく、かつ、CFBモードの初期状態である場合

8) 56ビット鍵モードではなく、かつ、CFBモードの定常状態である場合

これらの場合は、それぞれ5), 6)の場合と次の点を除いて同じである。すなわち、共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードではないことを示す信号が入力される。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードではないことを示す信号が入力されているので、入力された56ビットの鍵データKDのうち、必要がないビット（例えば上位16ビット）をマスクして、40ビット鍵データとしてECB処理器47に出力する。ECB処理器47は、ビットマスク器46から出力された40ビット鍵データを用いてECB処理を行う。

共用処理ブロック4の暗号化処理時の動作について、図2、図3の上段、及び

図4を参照して説明する。この場合、共用処理ブロック4には、暗号化／復号化切り替え信号SSとして、暗号化を示す信号が入力される。56ビット鍵モードであるか否か、CBCモード及びCFBモードのうちのいずれであるか、初期状態及び定常状態のうちのいずれであるかによって場合を分けて説明する。ECB処理器47におけるECB処理は、CBCモードの場合及びCFBモードの場合ともに暗号化処理である。

9) 56ビット鍵モードであり、かつ、CBCモードの初期状態である場合
(図4のENC-CBC Initの場合)

この場合は、図3の上段の処理E1及びその前の排他的論理和を求める処理が行われる。共用処理ブロック4は、入力された初期ベクタデータIVと暗号化されていないデータDとの排他的論理和を求めて、データIとして出力する。共用処理ブロック4は、得られたデータIにECB処理として「Encrypt」処理を行って、暗号化データCを求めて出力する。

この場合の処理を、図2を参照して説明する。共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードであること、及びCBCモードの初期状態であることを示す信号が入力される。

第1のセレクタ41は、処理ブロック入力データECを選択して出力する。第2のセレクタ42は、初期ベクタデータIVを選択して出力する。排他的論理和演算器49は、処理ブロック入力データECと初期ベクタデータIVとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データERを出力する。

第3のセレクタ43は、排他的論理和データERを選択してECB処理器47に出力する。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードであることを示す信号が入力されているので、入力された56ビットの鍵データKDをマスクせずにそのままECB処理器47に出力する。

ECB処理器47は、ビットマスク器46から出力された56ビット鍵データを用いて、第3のセレクタから出力された排他的論理和データERに対してECB処理として暗号化処理を行い、得られた暗号処理データPDを出力する。第4

のセレクトは、暗号処理データPDを選択して、処理済データDCとして暗号化結果を出力する。

10) 56ビット鍵モードであり、かつ、CBCモードの定常状態である場合(図4のENC-CBC Normalの場合)

この場合は、図3の上段の処理E2又はE3及びこれらのそれぞれの前の排他的論理和を求める処理が行われる。共用処理ブロック4は、暗号化されていないデータDとその前のECB処理で得られた暗号化データCとの排他的論理和を求めて、データIとして出力する。共用処理ブロック4は、得られたデータIにECB処理として「Encrypt」処理を行って、暗号化データCを求めて出力する。

この場合の処理を、図2を参照して説明する。共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードであること、及びCBCモードの定常状態であることを示す信号が入力される。

第1のセレクト41は、処理ブロック入力データECを選択して出力する。第2のセレクト42は、遅延器48が出力する遅延された暗号処理データPDDを選択して出力する。排他的論理和演算器49は、処理ブロック入力データECと遅延された暗号処理データPDDとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データERを出力する。

第3のセレクト43は、排他的論理和データERを選択してECB処理器47に出力する。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードであることを示す信号が入力されているので、入力された56ビットの鍵データKDをマスクせずにそのままECB処理器47に出力する。

ECB処理器47は、ビットマスク器46から出力された56ビット鍵データを用いて、第3のセレクトから出力された排他的論理和データERに対してECB処理として暗号化処理を行い、得られた暗号処理データPDを出力する。第4のセレクトは、暗号処理データPDを選択して、処理済データDCとして暗号化結果を出力する。

1 1) 5 6 ビット鍵モードではなく、かつ、C B Cモードの初期状態である場合

1 2) 5 6 ビット鍵モードではなく、かつ、C B Cモードの定常状態である場合

これらの場合は、それぞれ 9) , 1 0) の場合と次の点を除いて同じである。すなわち、共用処理ブロック 4 には、モード選択信号MSとして、5 6 ビット鍵モードではないことを示す信号が入力される。ビットマスク器 4 6 は、モード選択信号MSとして5 6 ビット鍵モードではないことを示す信号が入力されているので、入力された5 6 ビットの鍵データKDのうち、必要がないビット（例えば上位1 6 ビット）をマスクして、4 0 ビット鍵データとしてE C B処理器 4 7 に出力する。E C B処理器 4 7 は、ビットマスク器 4 6 から出力された4 0 ビット鍵データを用いてE C B処理を行う。

1 3) 5 6 ビット鍵モードであり、かつ、C F Bモードの初期状態である場合（図 4 のE N C - C F B I n i tの場合）

C F Bモードの処理のみを行うときには、C F Bモードの初期状態における処理が行われる。この場合は、図 3 の上段の処理E 9 及びこれに続く排他的論理和を求める処理が行われる。共用処理ブロック 4 は、暗号化されていないデータDを入力とし、「E n c r y p t」処理を行う。共用処理ブロック 4 は、この処理で求められたデータと入力された初期ベクタデータ I Vデータとの排他的論理和を求めて、暗号化データCとして出力する。

この場合の処理を、図 2 を参照して説明する。共用処理ブロック 4 には、モード選択信号MSとして、5 6 ビット鍵モードであること、及びC F Bモードの初期状態であることを示す信号が入力される。

第 1 のセレクタ 4 1 は、E C B処理器 4 7 が出力する暗号処理データ P Dを選択して出力する。第 2 のセレクタ 4 2 は、初期ベクタデータ I Vを選択して出力する。排他的論理和演算器 4 9 は、暗号処理データ P Dと初期ベクタデータ I Vとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データ E R

を出力する。

第3のセクタ43は、処理ブロック入力データECを選択してECB処理器47に出力する。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードであることを示す信号が入力されているので、入力された56ビットの鍵データKDをマスクせずにそのままECB処理器47に出力する。

ECB処理器47は、ビットマスク器46から出力された56ビット鍵データを用いて、第3のセクタから出力された処理ブロック入力データECに対してECB処理として暗号化処理を行い、得られた暗号処理データPDを出力する。第4のセクタは、排他的論理和演算器49が出力する排他的論理和データERを選択して、処理済データDCとして暗号化結果を出力する。

14) 56ビット鍵モードであり、かつ、CFBモードの定常状態である場合(図4のENC-CFB Normalの場合)

CBCモードの処理に続いてCFBモードの処理を行うときには、CFBモードの定常状態における処理が行われる。この場合は、図3の上段の処理E9及びこれに続く排他的論理和を求める処理が行われる。共用処理ブロック4は、その前のECB処理で得られた暗号化データCを入力とし、「Encrypt」処理を行う。共用処理ブロック4は、この処理で求められたデータと暗号化されていないデータDとの排他的論理和を求めて、暗号化データCとして出力する。

この場合の処理を、図2を参照して説明する。共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードであること、及びCFBモードの定常状態であることを示す信号が入力される。

第1のセクタ41は、ECB処理器47が出力する暗号処理データPDを選択して出力する。第2のセクタ42は、処理ブロック入力データECを選択して出力する。排他的論理和演算器49は、暗号処理データPDと処理ブロック入力データECとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データERを出力する。

第3のセクタ43は、遅延器48が出力する遅延された暗号処理データPD

Dを選択してECB処理器47に出力する。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードであることを示す信号が入力されているので、入力された56ビットの鍵データKDをマスクせずにそのままECB処理器47に出力する。

ECB処理器47は、ビットマスク器46から出力された56ビット鍵データを用いて、第3のセクタから出力された遅延された暗号処理データPDDに対してECB処理として暗号化処理を行い、得られた暗号処理データPDを出力する。第4のセクタは、排他的論理和演算器49が出力する排他的論理和データERを選択して、処理済データDCとして暗号化結果を出力する。

15) 56ビット鍵モードではなく、かつ、CFBモードの初期状態である場合

16) 56ビット鍵モードではなく、かつ、CFBモードの定常状態である場合

これらの場合は、それぞれ13)、14)の場合と次の点を除いて同じである。すなわち、共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードではないことを示す信号が入力される。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードではないことを示す信号が入力されているので、入力された56ビットの鍵データKDのうち、必要がないビット（例えば上位16ビット）をマスクして、40ビット鍵データとしてECB処理器47に出力する。ECB処理器47は、ビットマスク器46から出力された40ビット鍵データを用いてECB処理を行う。

なお、モード選択信号MSがECBモードを示す場合には、第3のセクタ43は処理ブロック入力データECを選択して出力し、かつ、第4のセクタ44は暗号処理データPDを選択して出力する。ECB処理器47は、暗号化／復号化切り替え信号SSが、暗号化を示す場合は暗号化処理を行い、復号化を示す場合は復号化処理を行う。すなわち、図1の暗号化復号化装置は、CBCモード及びCFBモードに加えてECBモードにおける暗号化及び復号化を行うことがで

きる。

また、56ビット鍵データ又は40ビット鍵データに代えて、他の長さの鍵データを用いるようにすることも容易にできる。

また、図1の暗号化復号化装置を暗号化装置として用いるようにしてもよい。この場合は、入力されたダウンストリームデータを暗号化して出力するのみでよく、以上の説明における復号化に対応した構成及び動作は不要である。また、暗号化／復号化切り替え信号SSは不要であり、第1～第4のセクタ及びECB処理器は、モード選択信号MSに従って動作すればよい。

より具体的には、遅延器は、暗号処理データPDを入力とし、これを遅延させて出力する。第2のセクタは、処理ブロック入力データEC、初期ベクタデータIV、及び遅延器が出力する遅延した暗号処理データPDDのうちのいずれかを選択して出力する。第3のセクタは、処理ブロック入力データEC、排他的論理和演算器が出力する排他的論理和データER、及び遅延した暗号処理データPDDのうちのいずれかを選択して出力する。第4のセクタは、暗号処理データPD及び排他的論理和データERのうちのいずれかを選択して、暗号化結果として出力する。

また、図1の暗号化復号化装置を復号化装置として用いるようにしてもよい。この場合は、入力されたアップストリームデータを復号化して出力するのみでよく、以上の説明における暗号化に対応した構成及び動作は不要である。このため、暗号処理データPDを常に出力する第1のセクタ、及び排他的論理和演算器が出力する排他的論理和データERを常に出力する第4のセクタは不要である。また、暗号化／復号化切り替え信号SSは不要であり、第2及び第3のセクタ及びECB処理器は、モード選択信号MSに従って動作すればよい。

より具体的には、遅延器は、処理ブロック入力データECを入力とし、これを遅延させて出力する。第2のセクタは、処理ブロック入力データEC、初期ベクタデータIV、及び遅延器が出力する遅延した処理ブロック入力データECDのうちのいずれかを選択して出力する。第3のセクタは、処理ブロック入力デ

ータEC、及び遅延した処理ブロック入力データECDのうちのいずれかを選択して出力する。排他的論理和演算器は、暗号処理データPDと第2のセレクタの出力との排他的論理和を求めて、復号化結果として出力する。

また、本発明は、CPUやDSP (digital signal processor) 等のプロセッサを用いたソフトウェアによる処理を行うことによって実現することも可能である。

以上のように、本発明に係る暗号化復号化装置によると、モード選択信号を変化させれば、ECBモード、CBCモード及びCFBモードのうちのいずれかと、56ビット鍵モード又は40ビット鍵モードのいずれかとを組み合わせたいずれのモードにおいても、同一のハードウェアによって暗号化データに対する復号化を行い、暗号解読データを得ることができる。

また、暗号化／復号化切り替え信号を変化させれば、いずれのモードにおいても、データの暗号化及び復号化のいずれをも、同一のハードウェアによって行うことができる。したがって、暗号化復号化装置の回路規模の削減を図ることができる。

図5は、本発明の実施形態に係る暗号化復号化装置の他の構成の例を示すブロック図である。図5の暗号化復号化装置は、データ構造解析ブロック202と、共用処理ブロック4と、データ制御ブロック206と、第1及び第2の入力セレクタ207、208と、出力セレクタ209とを備えている。図5の暗号化復号化装置は、トリプルDES (triple DES) 方式による暗号化及び復号化を行う装置である。共用処理ブロック4は、図1を参照して説明したものと同様のものである。

データ構造解析ブロック202は、図1のデータ構造解析ブロック2と同様の動作を行う他、入力されたストリームデータのヘッダから、このストリームデータをトリプルDES方式で処理すべきか否かを判断し、その結果をもTEK制御用データTKとしてデータ制御ブロック206に出力する。

データ制御ブロック206は、図1のデータ制御ブロック6と同様の動作を行

う他、TEK制御用データTKに基づいて、トリプルDES方式で暗号化又は復号化すべきである場合には、トリプルDESモードを示す信号をもモード選択信号MSとして共用処理ブロック4、入力セクタ207及び208に出力する。また、データ制御ブロック206は、出力制御信号OSを出力セクタ209に出力する。

入力セクタ207は、モード選択信号MSに従って、ダウンストリームデータSD又は共用処理ブロック4が出力する処理済データDCを選択し、データ構造解析ブロック202に出力する。入力セクタ208は、モード選択信号MSに従って、アップストリームデータSU又は処理済データDCを選択し、データ構造解析ブロック202に出力する。出力セクタ209は、出力制御信号OSに従って、処理済データDC又は値“0”を選択し、図5の暗号化復号化装置の処理済データTDとして出力する。

図5の暗号化復号化装置がトリプルDESモードで動作する際の動作について説明する。データ制御ブロック206は、通常は、ダウンストリームデータSD及びアップストリームデータSUをそれぞれ選択するように、入力セクタ207、208にモード選択信号MSを出力し、処理済データDCを選択するように、出力セクタ209に出力制御信号OSを出力する。

共用処理ブロック4は、入力されたダウンストリームデータSD又はアップストリームデータSUに対して1回目の処理を行い、処理済データDCを入力セクタ207、208、出力セクタ209に出力する。

モード選択信号MSがトリプルDESモードを示す場合には、入力セクタ207、208は、処理済データDCを選択する。このとき、出力セクタ209は、出力制御信号OSに従って、“0”を選択する。すると、共用処理ブロック4によって1回目の処理が行われた処理済データDCが、再びデータ構造解析ブロック202に inputs され、共用処理ブロック4によって2回目の処理が行われる。

入力セクタ207、208、出力セクタ209は、その後も同様の選択を行うので、共用処理ブロック4によって2回目の処理が行われた処理済データD

Cが、再びデータ構造解析ブロック202に入力され、共用処理ブロック4によって3回目の処理が行われる。

3回目の処理が終了すると、出力セクタ209は、処理済データDCを選択するので、トリプルDES方式で暗号化又は復号化の処理が行われた結果が処理済データTDとして出力される。このとき、入力セクタ207、208は、ダウンストリームデータSD及びアップストリームデータSUをそれぞれ選択する。共用処理ブロック4における3回の処理のそれぞれとしては、暗号化及び復号化のうちのいずれをも行うようにすることができる。特に、暗号化、復号化、暗号化の順に処理を行うと、トリプルDES方式による暗号化を行うことができ、復号化、暗号化、復号化の順に処理を行うと、トリプルDES方式による復号化を行うことができる。

このように、図5の暗号化復号化装置によると、共用処理ブロック4において暗号化又は復号化処理を3回行うので、トリプルDES方式による暗号化又は復号化を行うことができる。

なお、共用処理ブロック4における処理を、3回よりも多くの回数行うようにしてもよい。

図6は、図1の暗号化復号化装置を用いた送受信装置のブロック図である。図6の送受信装置100は、PHY部10と、MAC部20と、画像処理部32と、インタフェース部34と、チューナ52とを備えている。

PHY部10は、ダウンストリームPHY部11と、アップストリームPHY部12とを備えている。MAC部20は、ダウンストリームデータ処理部21と、アップストリームデータ処理部22と、暗号化復号化装置23、24と、CPU26と、記憶部28とを備えている。暗号化復号化装置23、24は、いずれも、図1の暗号化復号化装置と同様のものである。なお、暗号化復号化装置23、24として、図5の暗号化復号化装置を用いてもよい。

受信時には、チューナ52は、送信に使われるチャネルから1つを選択し、センタ装置80から送信された信号を低い周波数の信号に変換して、ダウンスト

リームPHY部11に出力する。ダウンストリームPHY部11は、受け取った信号をベースバンド信号に変換し、更にデータへの変換、及び誤り訂正を行って、ダウンストリームデータ処理部21に出力する。

ダウンストリームデータ処理部21は、受け取ったデータから、そのヘッダの情報に応じてダウンストリームデータSD、鍵データKD、初期ベクタデータIV等を分離して、暗号化復号化装置23に出力する。暗号化復号化装置23は、図1を参照して説明したように、暗号に対する復号化を行い、得られた処理済データDCをバス29に出力する。CPU26は、バス29を経由して、処理済データDCを記憶部28に格納させる。

CPU26は、記憶部28からデータを読み出し、画像処理部32に与える。画像処理部32は、受け取ったデータに対して画像として表示させるために必要な処理を行い、得られたデータをインタフェース部34を介して表示器（図示せず）に出力し、表示させる。

送信時には、CPU26は、記憶部28からデータを読み出し、バス29を経由して、暗号化復号化装置24にアップストリームデータSUとして与える。暗号化復号化装置24は、図1を参照して説明したように、受け取ったデータに対する暗号化を行い、得られた処理済データDCをアップストリームデータ処理部22に出力する。アップストリームデータ処理部22は、受け取ったデータにヘッダを付加する等の処理を行い、アップストリームPHY部12に出力する。アップストリームPHY部12は、受け取ったデータを電気信号に変換し、更にこれを送信に用いられる周波数に変換して、センタ装置80に送信する。

このように、図6の送受信装置によると、複数のモードにおける暗号化、又は複数のモードにおける復号化を、それぞれ同一のハードウェアによって行うので、回路規模の削減を図ることができる。

産業上の利用可能性

本発明に係る暗号化復号化装置及び方法は、多くの機能を低コストで提供する

ことができ、例えば、送受信装置や、データの記録再生装置等における暗号化及び暗号の復号化に有用である。

請 求 の 範 囲

1. 暗号化データ又は暗号化すべきデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、

前記処理ブロック入力データに対して前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する共用処理ブロックとを備え、

前記共用処理ブロックは、

入力された鍵データを用いたECB (electronic code book) 処理を行うこと
によって、CBC (cipher block chaining) モード及びCFB (cipher feedba
ck) モードのいずれにおいても暗号化及び復号化を行うことができるように構成
されており、前記モード選択信号に示されたモードで暗号化又は復号化を行うも
のである

暗号化復号化装置。

2. 請求項1に記載の暗号化復号化装置において、

前記データ構造解析ブロックは、

前記暗号化データにおけるヘッダの解析を行い、前記ヘッダの情報に基づいて
前記暗号化データからMAC (media access control) 構造を抜き出し、前記M
AC構造中に拡張ヘッダが存在し、かつ、前記拡張ヘッダに当該暗号化データが
暗号化されていることが示されている場合には、前記拡張ヘッダに含まれる暗号
化に関する情報を前記制御用データとして出力するとともに、前記MAC構造デ

ータから前記拡張ヘッダを除去して前記処理ブロック入力データとして出力するものである

ことを特徴とする暗号化復号化装置。

3. 請求項1に記載の暗号化復号化装置において、

前記データ制御ブロックは、

前記制御用データに従って、前記処理ブロック入力データをCBCモード、及びCFBモードのうちのいずれのモードで処理すべきか、並びにいずれの長さの鍵データを用いるモードで処理すべきかを示す信号を前記モード選択信号として出力するものである

ことを特徴とする暗号化復号化装置。

4. 請求項1に記載の暗号化復号化装置において、

前記共用処理ブロックは、

前記ECB処理を行い、得られた結果を暗号処理データとして出力するECB処理器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第1のセクタと、

前記処理ブロック入力データ、及び前記暗号処理データを入力とし、それぞれを遅延させて出力する遅延器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、並びに、前記遅延器が出力する遅延した処理ブロック入力データ及び遅延した暗号処理データのうちのいずれかを選択して出力する第2のセクタと、

前記第1のセクタの出力と前記第2のセクタの出力との排他的論理和を求めて出力する排他的論理和演算器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理和演算器の出力、前記遅延した処理ブロック入力データ、及び前記遅延した暗号処理データのうちのいずれかを選択して出力する第3のセレクトと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算器の出力のうちのいずれかを選択して、前記暗号化結果又は前記復号化結果として出力する第4のセレクトとを備え、

前記ECB処理器は、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記ECB処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第3のセレクトの出力に対して行い、得られた結果を前記暗号処理データとして出力するものであることを特徴とする暗号化復号化装置。

5. 請求項4に記載の暗号化復号化装置において、

前記ビットマスク器は、

前記モード選択信号が56ビット鍵モードであることを示す場合には、前記鍵データをそのまま、その他の場合には、必要がないビットをマスクして、前記モードに適合した鍵データとして出力するものであることを特徴とする暗号化復号化装置。

6. 請求項4に記載の暗号化復号化装置において、

前記第1のセレクトは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCBCモードであることを示す場合には、前

記処理ブロック入力データを選択して出力し、その他の場合には、前記暗号処理データを選択して出力するものであることを特徴とする暗号化復号化装置。

7. 請求項4に記載の暗号化復号化装置において、

前記第2のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCBCモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCFBモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCBCモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した処理ブロック入力データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCFBモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力するものである

ことを特徴とする暗号化復号化装置。

8. 請求項4に記載の暗号化復号化装置において、

前記第3のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であ

って、かつ、前記モード選択信号がC B Cモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC F Bモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC B Cモードであることを示す場合には、前記処理ブロック入力データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC F Bモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した処理ブロック入力データを選択して出力するものであることを特徴とする暗号化復号化装置。

9. 請求項4に記載の暗号化復号化装置において、

前記第4のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC B Cモードであることを示す場合には、前記暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC F Bモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合には、前記排他的論理和演算器の出力を選択して出力するものであることを特徴とする暗号化復号化装置。

10. 請求項4に記載の暗号化復号化装置において、
前記ECB処理器は、
前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合には、
暗号化処理を行い、
前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であ
って、かつ、前記モード選択信号がCBCモードであることを示す場合には、復
号化処理を行い、
前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であ
って、かつ、前記モード選択信号がCFBモードであることを示す場合には、暗
号化処理を行うものである
ことを特徴とする暗号化復号化装置。

11. 請求項1に記載の暗号化復号化装置において、
暗号化データ又は前記共用処理ブロックの出力を選択し、前記データ構造解析
ブロックに出力する第1の入力セクタと、
暗号化すべきデータ又は前記共用処理ブロックの出力を選択し、前記データ構
造解析ブロックに出力する第2の入力セクタと、
所定の値又は前記共用処理ブロックの出力を選択し、出力する出力セクタと
を更に備え、
前記暗号化データ又は前記暗号化すべきデータに対して前記共用処理ブロック
における処理が所定の回数行われると、前記出力セクタが前記共用処理ブロッ
クの出力を選択するように構成されている
ことを特徴とする暗号化復号化装置。

12. 請求項11に記載の暗号化復号化装置において、
前記所定の回数は、3回である
ことを特徴とする暗号化復号化装置。

13. 暗号化すべきデータを受け取り、そのデータ構造の解析を行って、制御データを求めて出力するとともに、前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、

前記処理ブロック入力データに対して暗号化を行い、得られた暗号化結果を出力する共用処理ブロックとを備え、

前記共用処理ブロックは、

入力された鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても暗号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化を行うものである暗号化装置。

14. 請求項13に記載の暗号化装置において、

前記共用処理ブロックは、

前記ECB処理を行い、得られた結果を暗号処理データとして出力するECB処理器と、

前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第1のセレクタと、

前記暗号処理データを入力とし、これを遅延させて出力する遅延器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延器が出力する遅延した暗号処理データのうちのいずれかを選択して出力する第2のセレクタと、

前記第1のセレクタの出力と前記第2のセレクタの出力との排他的論理和を求めて出力する排他的論理和演算器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理

和演算器の出力、及び前記遅延した暗号処理データのうちのいずれかを選択して出力する第3のセレクトと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、

前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算器の出力のうちのいずれかを選択して、前記暗号化結果として出力する第4のセレクトとを備え、

前記ECB処理器は、

前記ECB処理として暗号化処理を前記モードに適合した鍵データを用いて前記第3のセレクトの出力に対して行い、得られた結果を前記暗号処理データとして出力するものであることを特徴とする暗号化装置。

15. 暗号化データを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、

前記処理ブロック入力データに対して復号化を行い、得られた復号化結果を出力する共用処理ブロックとを備え、

前記共用処理ブロックは、

入力された鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで復号化を行うものである復号化装置。

16. 請求項15に記載の復号化装置において、

前記共用処理ブロックは、

前記ECB処理を行い、得られた結果を暗号処理データとして出力するECB処理器と、

前記処理ブロック入力データを入力とし、これを遅延させて出力する遅延器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延器が出力する遅延した処理ブロック入力データのうちのいずれかを選択して出力する第2のセレクタと、

前記暗号処理データと前記第2のセレクタの出力との排他的論理和を求めて、前記復号化結果として出力する排他的論理和演算器と、

前記モード選択信号に従って、前記処理ブロック入力データ、及び前記遅延した処理ブロック入力データのうちのいずれかを選択して出力する第3のセレクタと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器とを備え、

前記ECB処理器は、

前記モード選択信号に従って、前記ECB処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第3のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

ことを特徴とする復号化装置。

17. 受信した信号をデータに変換して出力するダウンストリームPHY部と、

前記データからダウンストリームデータ及び鍵データを分離して出力するダウンストリームデータ処理部と、

前記鍵データを用いて前記ダウンストリームデータを復号化して出力する第1の暗号化復号化装置と、

前記復号化されたダウンストリームデータを格納する記憶部と、

前記記憶部から読み出されたアップストリームデータを暗号化して出力する第2の暗号化復号化装置と、

前記暗号化されたアップストリームデータに、暗号化に用いられた鍵データを付加して出力するアップストリームデータ処理部と、

前記アップストリームデータ処理部が出力するデータを信号に変換して送信するアップストリームPHY部とを備え、

前記第1及び第2の暗号化復号化装置は、いずれも、

暗号化データを含む前記ダウンストリームデータ又は暗号化すべきデータを含む前記アップストリームデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、

前記処理ブロック入力データに対して前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する共用処理ブロックとを有するものであり、

前記共用処理ブロックは、

入力された鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化又は復号化を行うものである

送受信装置。

18. 暗号化データ又は暗号化すべきデータのデータ構造の解析を行って、

暗号化に関する情報を制御用データとして求めるとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして求めるデータ構造解析ステップと、

前記制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替えデータと、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データとを求めるデータ制御ステップと、

前記処理ブロック入力データに対して前記暗号化／復号化切り替えデータに従って暗号化又は復号化を行って、暗号化結果又は復号化結果を求める共用処理ステップとを備え、

前記共用処理ステップは、

鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても暗号化及び復号化を行うものであり、前記モード選択データに示されたモードで暗号化又は復号化を行うものである
暗号化復号化方法。

19. 暗号化すべきデータのデータ構造の解析を行って、制御用データを求めるとともに、前記暗号化すべきデータを処理ブロック入力データとして求めるデータ構造解析ステップと、

前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データを求めるデータ制御ステップと、

前記処理ブロック入力データに対して暗号化を行って、暗号化結果を求める共用処理ステップとを備え、

前記共用処理ステップは、

鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても暗号化を行うことができるものであり、前記モード選択データに示されたモードで暗号化を行うものである
暗号化方法。

20. 暗号化データのデータ構造の解析を行って、暗号化に関する情報を制御用データとして求めるとともに、前記暗号化データを処理ブロック入力データとして求めるデータ構造解析ステップと、

前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データを求めて出力するデータ制御ステップと、

前記処理ブロック入力データに対して復号化を行って、復号化結果を求める共用処理ステップとを備え、

前記共用処理ステップは、

鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても復号化を行うことができるものであり、前記モード選択データに示されたモードで復号化を行うものである
復号化方法。

1/6

FIG. 1

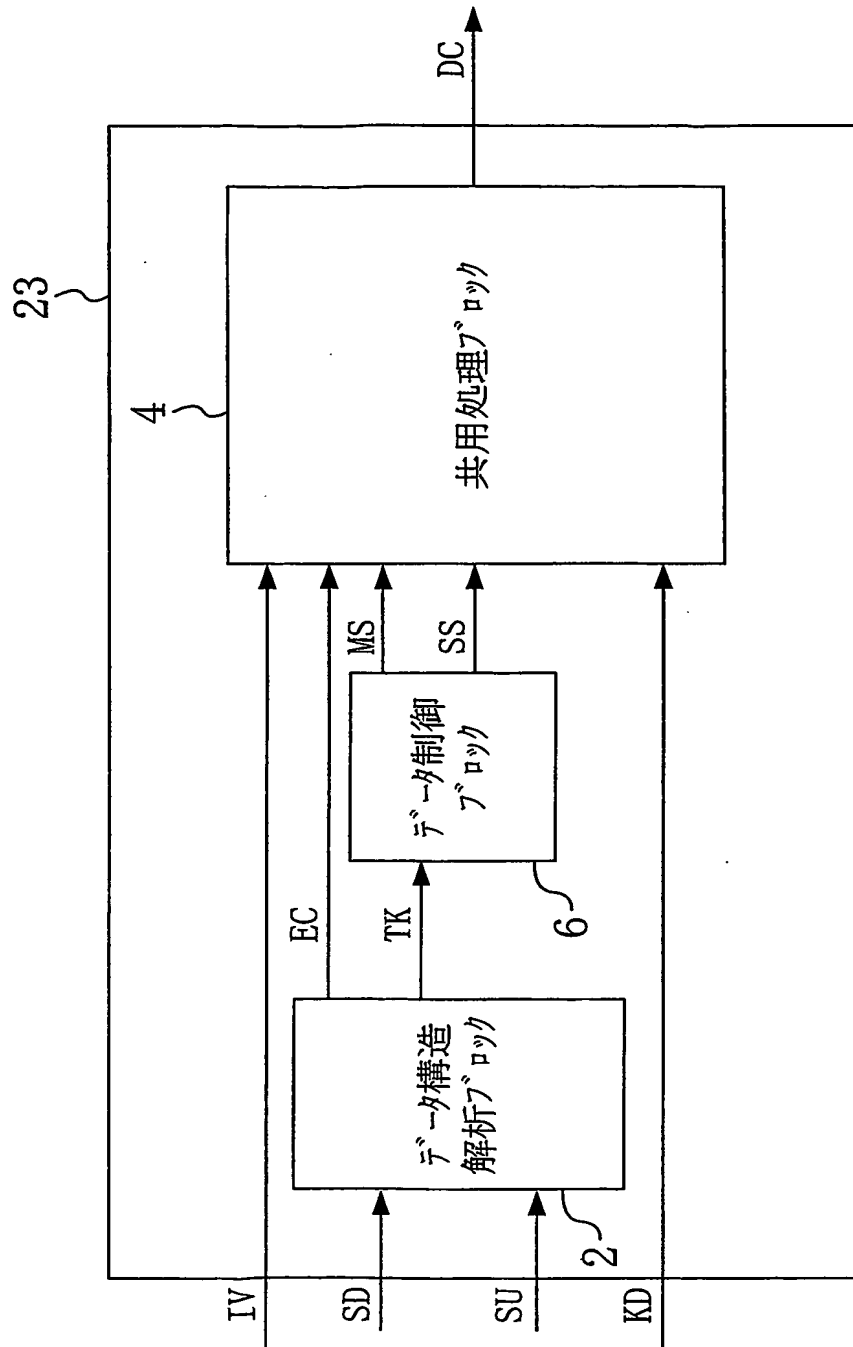


FIG. 2

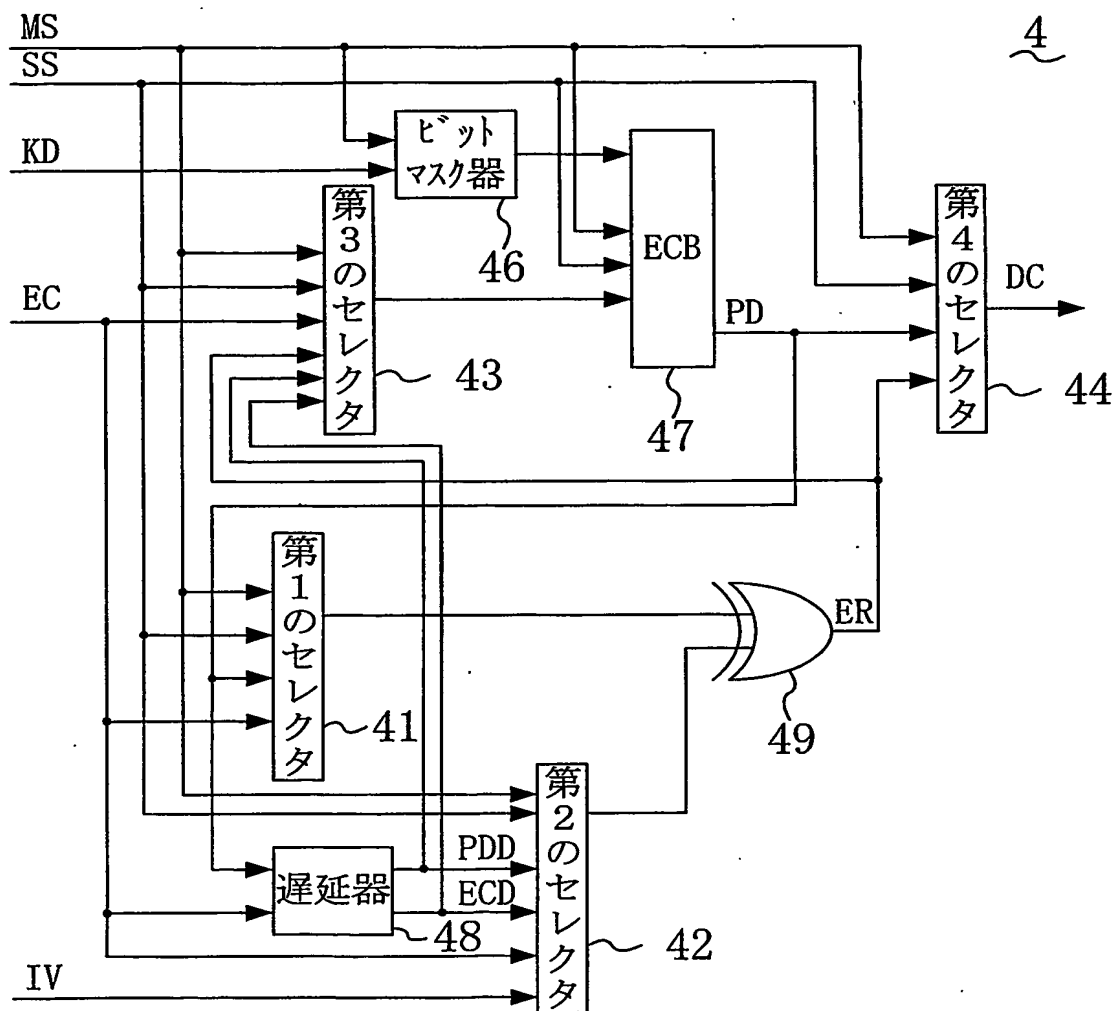


FIG. 3

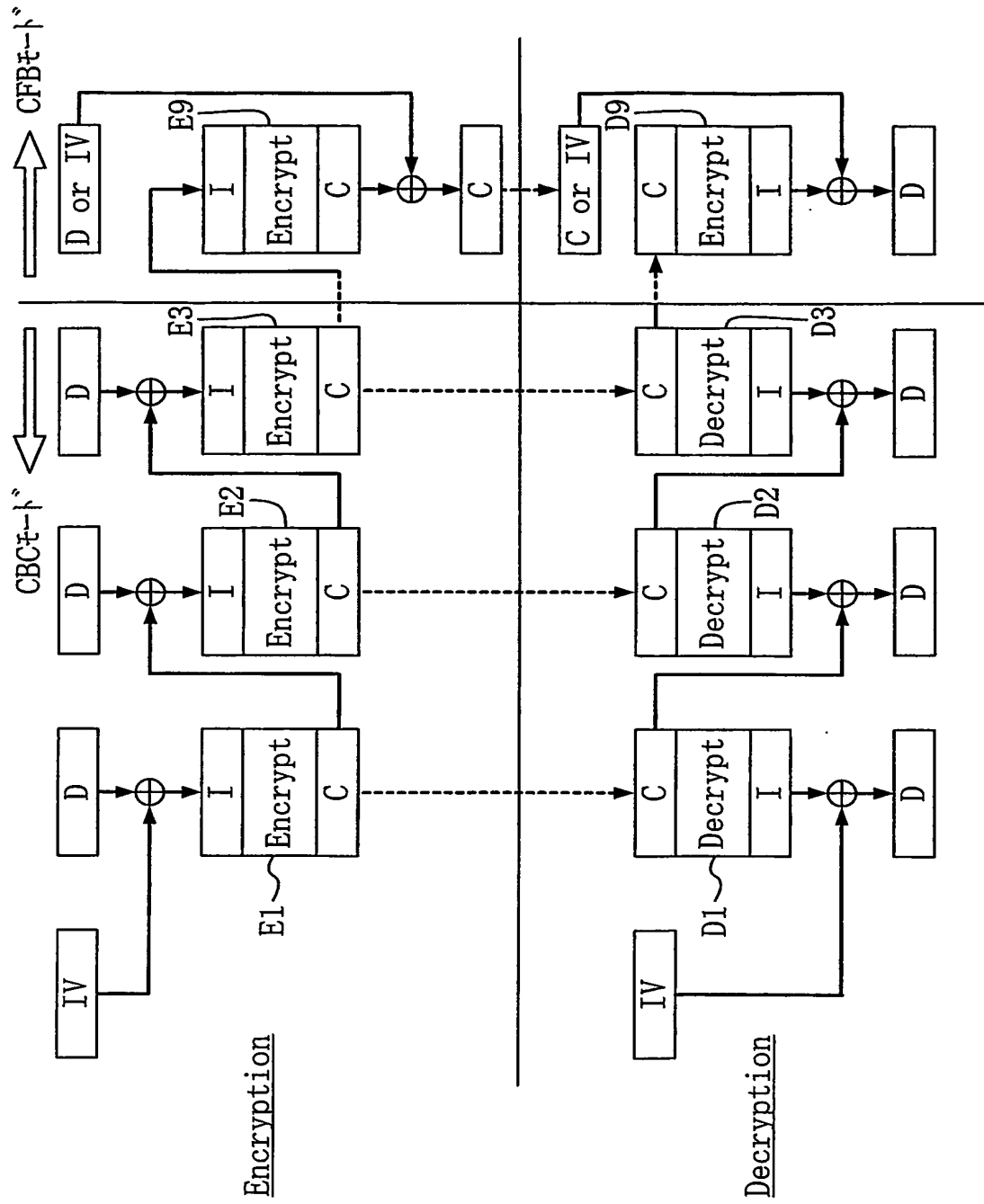


FIG. 4

	DEC-CBC Init	DEC-CBC Normal	DEC-CFB Init	DEC-CFB Normal	ENC-CBC Init	ENC-CBC Normal	ENC-CFB Init	ENC-CFB Normal
第1のセクタ	PD	PD	PD	PD	EC	EC	PD	PD
第2のセクタ	IV	ECD	IV	EC	IV	PDD	IV	EC
第3のセクタ	EC	EC	EC	ECD	ER	ER	EC	PDD
第4のセクタ	ER	ER	ER	ER	PD	PD	ER	ER

FIG. 5

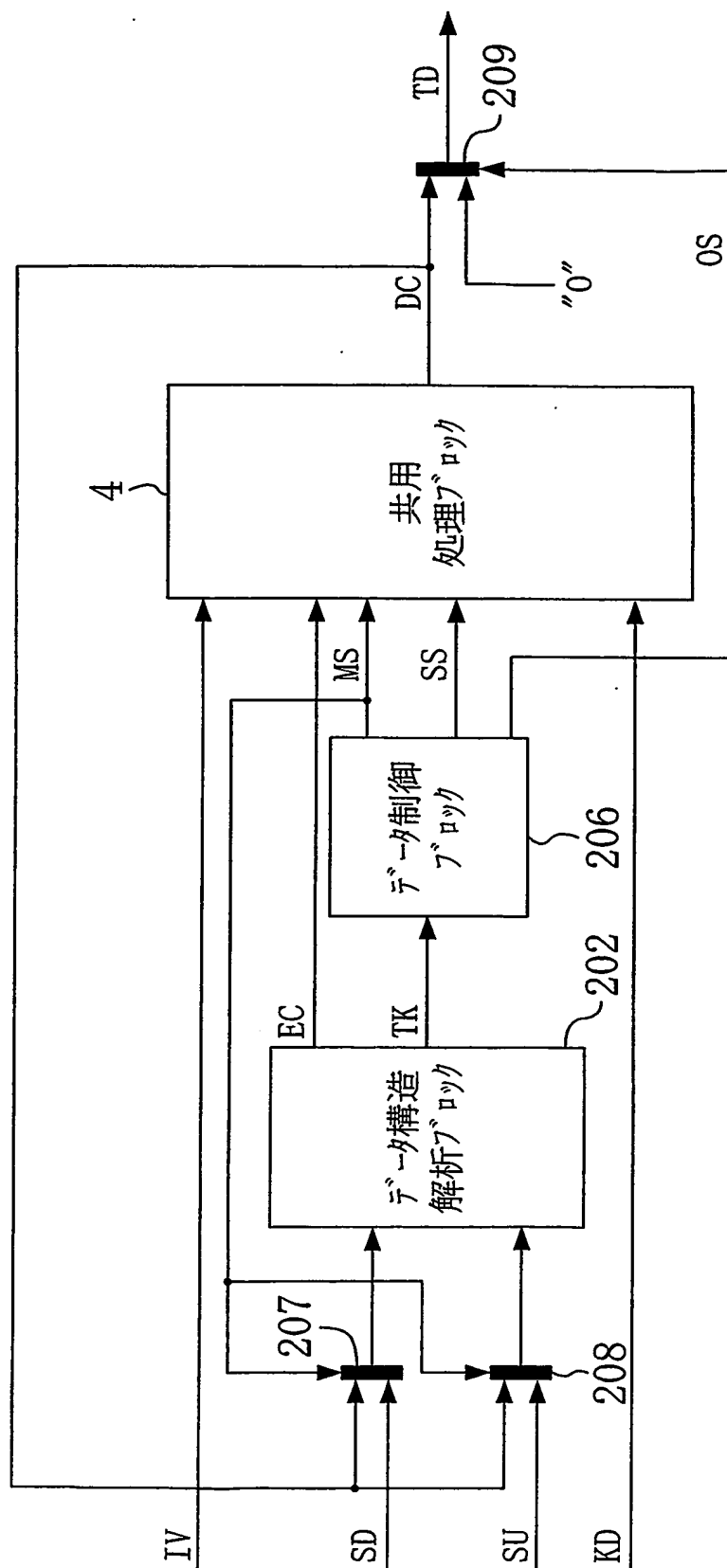
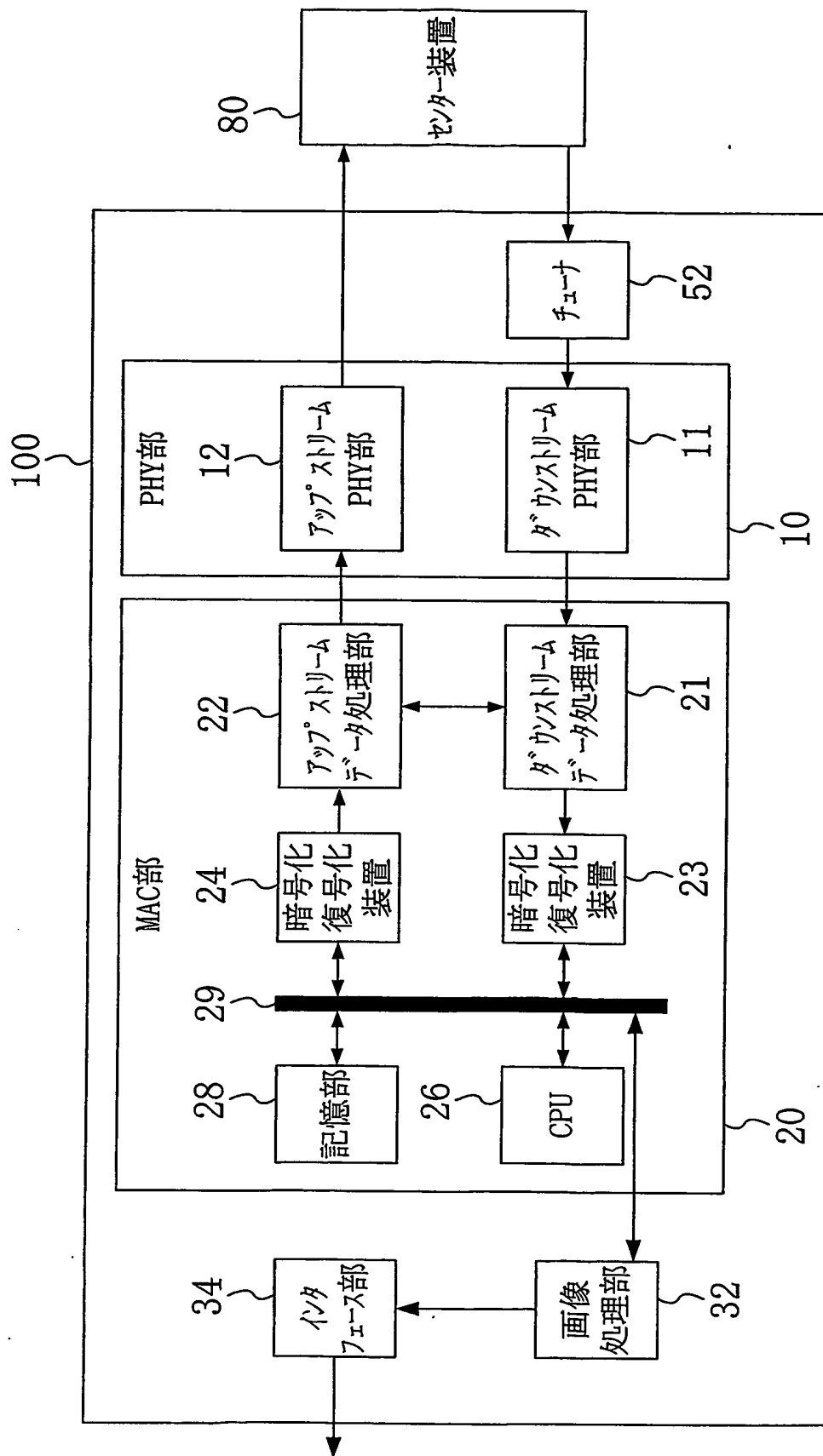


FIG. 6



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/10186

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/06, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/06, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2000-75785 A (Fujitsu Ltd.), 14 March, 2000 (14.03.00),	1, 13, 15, 17-20
Y	Full text	2, 3
A	(Family: none)	4-12, 14, 16
X	JP 7-261662 A (Fujitsu Ltd.), 13 October, 1995 (13.10.95),	1, 13, 15, 17-20
Y	Full text	2, 3
A	(Family: none)	4-12, 14, 16
Y	JP 2001-177518 A (NEC Corp.), 29 June, 2001 (29.06.01), Full text (Family: none)	2, 3

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
28 October, 2003 (28.10.03)Date of mailing of the international search report
11 November, 2003 (11.11.03)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/10186

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-215244 A (Sony Corp.), 11 August, 1998 (11.08.98), Full text (Family: none)	2
P, X	JP 2002-297030 A (Toshiba Corp.), 09 October, 2002 (09.10.02), Full text (Family: none)	1, 13, 15, 17-20

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L 9/06, G09C 1/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L 9/06, G09C 1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2003年
 日本国登録実用新案公報 1994-2003年
 日本国実用新案登録公報 1996-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y A	J P 2000-75785 A (富士通株式会社) 2000.03.14, 全文 (ファミリーなし)	1, 13, 15, 17-20 2, 3 4-12, 14, 16
X Y A	J P 7-261662 A (富士通株式会社) 1995.10.13, 全文 (ファミリーなし)	1, 13, 15, 17-20 2, 3 4-12, 14, 16

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

28.10.03

国際調査報告の発送日

28.10.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

石田 信行



5M

9469

電話番号 03-3581-1101 内線 3598

C (続き). 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2001-177518 A (日本電気株式会社) 2001. 06. 29, 全文 (ファミリーなし)	2, 3
Y	JP 10-215244 A (ソニー株式会社) 1998. 08. 11, 全文 (ファミリーなし)	2
PX	JP 2002-297030 A (株式会社東芝) 2002. 10. 09, 全文 (ファミリーなし)	1, 13, 15, 17-20